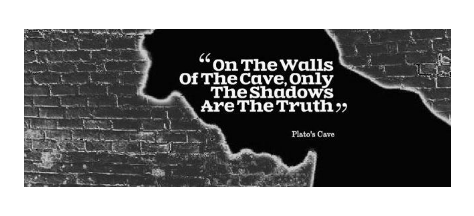
Become a member Sign in Get started

解密文件：科技产业巨头为什么能成为巨头？私有化间谍活动如何发动了认知战争？

iYouPort Follow
Jul 25, 2018 · 25 min read

“今天主宰智能行业的许多公司都是当年通过向情报界提供技术服务和产品而开始的（否则他们没有今天这般强大）”，“大多数情报工作不是由政府机构执行的，而是私人情报公司，而且大部分工作涉及情报工作的另一个共同方面：欺骗”……



这里其实是两篇文章，我们将它们放在一起是为了说明，私有化间谍活动并非只有情报信息“安全性”的问题，还有操纵的问题。今天的大多数情报工作不是由政府机构执行，而是由私人情报公司执行，而且大部分工作都会涉及情报工作的另一个共同方面：**欺骗**。

也就是说，它不仅涉及隐藏现实，还涉及**制造现实 —— 制造符合当权者利益的“现实“**。后面一篇文章为纽约时报的揭露，情报机构借手承包商操纵社会舆论、抹黑说出真相的人。

此前不久有新闻称，中国正在考虑“警务外包”，目前没有具体细节被公开。但这一趋势似乎不是虚晃，众所周知中国一直在效仿美国的所有弊端（一点优点都没学到）利用其发展自己的帝国路线，同时作为民族主义护盾。我们希望本文能帮助中国人理解私有化间谍活动的深意，以及公民社会应该如何利用基本知情权寻求真相。

欢迎来到 Matrix 的世界！不幸的事，这不是电影。

美国是许多国际情报共享的缔约国，其中最突出的就是所谓的“五眼”联盟。

五眼联盟诞生于第二次世界大战期间的间谍工作布局，促进了美国、英国、澳大利亚、加拿大和新西兰之间信号情报的共享。五眼国家同意默认交换他们收集的所有情报，以及与信号情报操作相关的方法和技术。当五眼第一次同意这种情报交换 —— 在第一条跨大西洋电话线铺设之前 —— 他们几乎没有预料到今天等待他们的技术进步。

然而，我们仍然对目前关于五眼之间情报共享的法律框架一无所知，包括美国政府获取的信息类型、**管理美国情报机构的信息获取、和传播大众私人通信和数据的规则**。

2017 年 7 月，隐私国际组织和耶鲁大学法学院的媒体自由和信息访问研究所，向国家安全局、国家情报局局长办公室、国务院和国家档案与记录管理局提起诉讼，根据信息自由法案，要求查阅有关五眼联盟的记录。

足足等了一年，也就是才刚，隐私国际组织开始接受国家安全局和国务院的**有限披露**。虽然还没有看到当前协议的文本，以及其他会对协议如何运作有重要启示的记录 — 但迄今为止的披露已经能使人们能够更为深入地了解美国情报共享协议的性质和范围。

本报告将总结其中的一些披露，并讨论它们的含义。重点研究其中一项协议 — 1961 年美国政府与英国政府之间的“一般安全协定” —— 此处进一步验证了我们对情报活动私有化的理解，并提供了一个难得的观察视角：关于 **“第三方统治”，这是对情报共享的监督和问责的明显障碍**。

延伸阅读：1959–61 英国— 美国通信情报（UKUSA）协议附录

披露

支持五眼联盟的情报分享安排首先被记录在英国和美国在 1946 年的通信情报协议中，后来改名为 UK-US 通信情报协议。在隐私国际组织提起诉讼的时候，该协议的 1956 年版本是最新公开的。为了回应诉讼，国家安全局披露了几个跨越 1956 年至 1961 年的附录，因此也更新了对该协议的理解。

这里是英文版：1961 General Security Agreement between the Government of the United States and the Government of the United Kingdom (General Security Agreement)

国务院披露了“一般安全协议”以及为执行该协议条款而制定的一套程序。“一般安全协定”涉及保护美国和英国之间交换的机密信息，并规定“由两国政府中的任何一方给予安全分类的信息……任何一方政府通过政府渠道向另一方提供的服务将按照这些分类进行……接收方政府将确保一定程度的保护，相当于或大于提供资料的政府所要求的保护程度。”国务院还披露了一些换文，当时的英国大使给美国大使 Harold Caccia 的信息、美国国务卿 Dean Rusk 表示各自政府接受协议条款。

这里是英文版：1998 Agreement to Extend the 1966 Agreement between the Government of Australia and the Government of the United States of America relating to the Establishment of a Joint Defence Facility at Pine Gap (Pine Gap Agreement)

美国国务院披露了当时的澳大利亚外交部长 Alexander Downer 和当时的美国大使之间的换文。澳大利亚大使 Genta Holmes 表示各自政府同意延长 1966 年“澳大利亚政府与美国政府关于在 Pine Gap 建立联合防御设施协定”的条款。

Pine Gap 是一个位于澳大利亚 Alice Springs 的基地，由美国和澳大利亚共同运营。**在 Pine Gap 美国控制着跨越几大洲的卫星，这些卫星可以监视无线通信，例如通过手机、无线电和卫星上行链路传输的无线通信。收集的情报支持情报活动和军事行动，包括无人机空袭。**

这些披露的文件表明，美国和澳大利亚政府同意将“Pine Gap 协定”**从 1998 年11月16日起“延长十年”的协议，并在此后继续有效“直至终止”**。Downer 对 Holmes 的来信明确提出了这点：

> this Note and your confirmatory reply thereto shall together constitute an Agreement between our two Governments concerning this matter which shall enter into force on the date that the Government of Australia notifies the Government of the United States of America that all domestic procedures as are necessary to give effect to this Agreement in Australia have been satisfied.

意见

上述的 Pine Gap 协定和“一般安全协议”在一个值得注意的方面有所不同：虽然美国公众可以获知 1998 年 Pine Gap 协定的延期，但 1961 年的“一般安全协议”尚未由美国公布。这种差异揭示了要求公布国际协议的相关法律中的差距。并且它支持在其他地方提出的呼吁，要求在这些类型的协议的形成和法律基础上提高行政部门的透明度和问责制。

美国明确认为 1998 年对 Pine Gap 协议的延期是一项具有法律约束力的国际协议。美国国务院在条约和其他国际协议系列（TIAS）中公布了 1998 年的 Pine Gap 协议，该系列作为美国签订的条约和其他国际协议的“有力证据”。同样，澳大利亚政府在澳大利亚条约系列中发布了 Pine Gap 协议。但是，**尽管澳大利亚政府还公布了原始的 1966 年 Pine Gap 协议的文本，但美国却没有**。

这一遗漏很重要，因为只有 1966 年的协议包含双方商定的条款 —— 换言之，建立联合防御设施以开展情报活动的协议的性质和范围。

同样，美国和英国似乎都没有公布1961年的“一般安全协议”。根据美国政府 2000 年对议会问题的答复，当时的总安全协议尚未解密。通过各种公开的材料，包括政府网站和学术数据库，隐私国际组织发现了几个对一般安全协议的引用，但没有提到协议本身（也没有部分内容）。例如，2007 年“英国关于国防贸易合作条约”承认“根据”一般安全协议“制定的原则”……但是，公民社会组织在国务院根据 FOIA 要求披露之前，没人知道这些原则是什么。

有一个明显的论点是，国家有法律义务公布 Pine Gap 协定的原始文本和 1966 年的“一般安全协议”，以及对两者的任何更新。根据 1 U.S.C. §112a，国务大臣必须公布美国加入的所有条约和非条约国际协定。**但这项义务受第112a（b）段中列出的一系列例外情况的限制。最值得注意的是，如果“总统认为”披露会损害国家安全利益，国务院就可以选择不披露。**

政府可以证明其未能公布协议的理由有两个。首先，国家安全豁免可能适用。然而，鉴于最初的 Pine Gap 协议已经由澳大利亚政府和联合国公布，并且国家根据信息自由法的要求发布了“一般安全协议”。

可以提出的第二个论点是，美国国务院并未认为 1966 年 Pine Gap 的协定和一般安全协议是具有约束力的国际协议。根据现行美国法律，具有法律约束力的国际协议可采取条约或执行协议的形式。大多数美国国际协议都是执行协议，正如国会研究处概述的那样，它采取三种一般形式：

> （1）国会 — 执行协议，其中，国会提前或追溯授权执行机构签订的国际协议；（2）根据早先条约签订的执行协议，其中协议由批准的条约授权；（3）唯一执行协议，其中根据总统的宪法授权而未经国会授权进行协议。

1966 年 Pine Gap 协定和“一般安全协议”似乎属于第三类。两者均根据行政部门在外交和国家安全方面的 Article II 权力而未经国会授权而建立。

在20世纪70年代之前，执行协议是不受管制和未定义的。事实上，直到 1971 年 Case-Zablocki 法案通过后，国务院才概述了非条约国际协议的标准。按照这种逻辑，美国没有公布这些协议是因为不理解他们在签署时触发了 §112a 的发布要求。

然而，**这一论点是可疑的，因为这两项协议似乎仍然有效。事实上，有证据表明，1966 年的一般安全协议并非最新版本**。英国下议院提到 1983 年和 1984 年对“一般安全协定”的修正案，以及“英国国防部和美国国防部之间运作的新安全实施安排”，建立于 2003 年。由于是国务院提供了这些披露，因此足证国家拥有这些协议（甚至承认 TIAS 中的 Pine Gap 协议）。因此，国务院有必要根据 §112a 公布协议。

美国政府未能公布这些协议，加剧了长期以来对美国法律下的国际协议的构成、法律依据、已形成的数量、以及它们包含的内容的混乱认识，这也使公众更难以向政府提出承责要求。

正如其他人所指出的那样，“今天几乎所有的美国国际法律都是由总统单独指挥行动的，而国会或美国公众几乎没有任何监督权。”简而言之，公众成员不应该进行冗长的 FOIA 程序才能揭示支持人们对国家安全和国际合作的理解的协议文本。（本报告的这些披露是在隐私国际组织提出请求后将近一年的时间才获得的）

1961 年的一般安全协议

下面将仔细研究 1961 年的一般安全协议。特别是，**考虑其关于私人承包商作用的规定，这有助于理解情报活动的私有化。进一步考虑“一般安全协议”援引“第三方规则”，这是情报共享协议中一个鲜为人知的但却很常见的特征，它对情报共享的有效监督和问责制提出了挑战。**

私有化间谍活动的历史

1961 年“一般安全协定”重点阐述了间谍私有化的历史和范围。特别是在美国情报界的形成时期。关于这一主题的大量文献确实存在，其中一个主要的例子是 Tim Shorrock 的“Spies for Hire,”。其中讨论了“**美国情报 — 工业联合体**，它所服务的机构，其主要的工业企业，以及经营其最大公司的前高级国家安全官员。”

在他的书中，Shorrock 绘制了这种伙伴关系的历史渊源和规模。例如，他描述了中央情报局如何与洛克希德公司签订合同，建造用于在冷战期间收集情报的 U-2 间谍飞机。他还描述了中央情报局与通用电气、Itek 和洛克希德公司签订的 CORONA 侦察卫星的委托合同，该卫星编制了苏联洲际弹道导弹复合体。

中央情报局并不是这种伙伴关系中唯一的政府参与者。正如 Shorrock 所强调的那样，**“外包一直是美国间谍事业的一部分”。这表明美国情报界的其他部门长期以来一直参与这项工作。**

例如，在 20 世纪 50 年代，IBM、贝尔实验室和 Cray 开发了第一台超级计算机和加密设备，NSA “用它来破解外交和军事信息，并将大量的信号转换为可操作的情报。”

现有的大部分文献都集中在美国情报界和美国公司之间的关系上，但很少有人知道，从美国国家情报机构到外包的外国公司，再从外国政府到美国公司的状况。人们对外国承包商向美国情报的机密信息获取了解甚少。“一般安全协定”的“产业安全附件”阐明了这些关系：

附件管辖“合同、分包合同、预先谈判、或其他政府批准的安排涉及其中一个或两个国家的机密信息的案例”，以下简称机密合同，由“美国或英国的”或“代表美国或英国政府”下达或签署。

附件提供了一种机制，通过该机制，**美国或英国的承包商可以被视为政府实体，以便共享机密信息**。一般规则是“机密信息和材料的传输只能通过每个政府指定的代表进行，即通过经授权的政府渠道进行传播。”但是：

有例外。美国可以将机密材料直接传送给位于美国的公司，该公司在美国实体的所有权、控制权或影响力之下，英国可以将此类信息直接传送给英国的公司，该公司在英国实体的所有权、控制权、或影响力之下，只要这些公司获得了相应的安全许可。

附件还提供了一种非美国/英国的机制，承包商可能“有资格获得机密合同”的一般规则是“在第三方国家的所有权、控制权或影响力之下的企业不符合条件，”但是“允许释放信息的政府考虑例外情况”。

Shorrock 指出，**“今天主宰智能行业的许多公司都是当年通过向情报界提供技术服务和产品而开始的（否则他们没有今天这般的强大）”**。因此，**传感器点认为，20 世纪 50 年代和 60 年代的公私伙伴关系主要是技术性的 —— 即促进新的监视能力的发展。**

延伸阅读：如果您曾经对这篇文章感觉疑惑（互联网究竟是什么），那么现在应该理解了，硅谷巨头之所以成为巨头，是因为他们一直服务于情报部门为其充当伙伴和合谋者；我们在这篇文章中有一个比较全球性视角的描述（公私监控伙伴关系）

因此，人们希望“产业安全附件”将承包商的活动范围限制在完成这些技术任务所必需的信息范围内。但实际上，附件对可能与承包商共享的信息类型没有任何限制。相反，附件涵盖了“任何形式的机密信息，无论是口头的，可视的的还是文字材料形式的”，并将材料定义为“一切，无论其物理性质或构成如何”，包括文件、书写、地图和信件。

此外，附件也没有规定情报情报活动可以外包的标准，是否可以外包给外国承包商，以及在什么情况下可以外包。

过去，学者们曾经对间谍工作私有化提出过担忧。例如，Martin Trybus 教授认为，将情报工作私有化会产生一系列基本目标：

> 首先，民主和法治受到损害。透露议会和司法的审查首先就是实现私有化的重要原因：其次，**由于私营部门的成本较高，于是不再得有所惠**，而且安全审批的必要性限制了竞争，在一定程度上破坏了在资本市场中的分配和保密间题主导的面向部门私有化的经济理由；最后，**国家安全——存在泄密风险被情报成本的影响，另一方面情报和技术读窃被转移到了情报机构之外……**

间谍活动的私有化也引起了人们对本土政府职能外包的担忧。美国法律长期以来一直禁止政府机构外包“本质上属于政府职能”，关于什么构成了“固有的政府职能”的指导不足（有关美国法律中相互矛盾的定义的审查，请参阅国会研究处2009年的摘要）。比如是否应允许私人承包商进行目标选择或情报分析与核查？

Simon Chesterman 教授指出，“这方面的不确定性似乎是故意的，从而加剧了保密性所带来的对问责制的挑战。”

“第三方规则”或“发起人控制原则”

1961 年的一般安全协议也提供了对“第三方规则”或“创始人控制原则”的罕见视角。被认为是许多情报共享安排的共同特征，第三方规则禁止在未经信息来源所有国事先同意的情况下，将机构之间共享的信息披露给第三方（可能包括监督机构）。正如隐私国际所指出的，**此类规则限制了监督行使对情报共享的责任**。

虽然在民间社会和各协组织的情报共享讨论中经常使用第三方规则，但人们几乎没有机会查阅规则在实际中的实际情况，因为情报共享协议很少受到公众监督的影响。“一般安全协议”包含第三方规则的两种不同表述：一种包含在信函交换中，涉及美国与英国的协议，另一种包含在“一般安全程序协议”的附件中，前者比后者更具有实力，也更不怎么严谨。内容如下：

> 认识到保护我们政府之间直接或间接传达的所有机密信息对我们两国的国家安全和保障至关重要，我谨建议以下方面为相互理解和保护这些信息，即接收方：a. 未经发送方政府的批准，不会将信息发布给第三国政府；b. 将承诺向发送方政府提供与其提供的保护程度基本相当的信息；c. 除非已给出的具体目的，不会使用该信息用于其他目的；d. 将尊重信息中涉及的私人权利，例如专利、版权或商业秘密。”（重点补充）

附件中表达的第三方规则要短得多，只是指出：“受援国政府不会将此类信息用于其他目的，并且未经事先同意不会将此类信息透露给第三国政府”。

正如所阐述的那样，第三方规则表明了合作伙伴机构希望保留对其共享信息的某种程度的控制。在某些情况下，这种控制愿望也可能保护人权。例如，该规则有助于防止向第三方机构进一步传播共享信息，特别是那些可能会滥用信息的机构。

但一个被误用的例子是 Maher Arar 案，加拿大政府在此案中提供了不准确的情报，后来与美国政府分享。美国政府随后将 Arar 先生拘留了 12 天，然后继续让他在叙利亚遭受酷刑的折磨。

政府还将第三方规则解释为禁止向其他第三方披露，**并将监督机构也被纳入了该禁令。根据这种解释，即使监督规则可能从根本上就不利于情报监督。**

作为一项原则问题，要求监督机构寻求外国机构的同意，以获取与国内机构共享的情报信息，这将削弱其行使独立和公正监督的能力，而且作为一种惯例，外国合作伙伴不大可能同意这种要求。“一般安全协议”中第三方规则的两种不同表述突出表明，该规则没有“通用标准”的用语。关注人权规则的替代版本至少应该包括，例如，一个明确允许两国监督机构审查共享信息的架构。

— — The Real War on Reality — —

以下是纽约时报 2013 年的报道，揭示了**私有化间谍活动在操纵社会舆论中发挥的作用。**

这篇报道发表在 Snowden 的曝光之后不久，当时随随着媒体参与到该史上最大规律的揭露中来，真相已经无法掩饰，于是当局启动操纵舆论的方法，尝试尽可能减轻问责的压力，**这种操纵就是通过互联网实现的。**

当时，“美国是大规模监控公民的国家”这一概念已经深入人心，舆论停留在关于国家安全局 PRISM 数据收集计划的启示上，但忽略了另一个事实 —— **今天的大多数情报工作不是由政府机构执行的，而是由私人情报公司执行，而且大部分工作涉及情报工作的另一个共同方面：欺骗**。

也就是说，不仅涉及隐藏现实，还涉及“制造现实” —— 制造符合当权者利益的“现实”。监视收集的目的是操纵。

纽约时报说，阴暗面强大的力量中的秘密和欺骗问题可能起来像是惊悚片，但它也是哲学家的工作。更准确地说，理解欺骗及其如何暴露是过去 2500 年来哲学的一个主要课题。也是一个记者、哲学家和其他所有寻求真相的人所从事的工作可以发生触碰的地方。

在西方知识传统中最常引用的一个寓言是柏拉图。他描述了一群人在洞穴内被锁住，背后有一个火堆。他们只能看到走在他们身后的人在墙上投下的阴影。他们把阴影误认为是“现实”。如何摆脱这种困境看到真实存在的东西？这些人需要不受束缚并走出洞穴才行。

报告真实存在于在洞穴之外的世界，是哲学家的基本职责之一。

在更现代的意义上，还应该考虑完全保密的运作该种模式作为认识论中的一个问题领域，其用来创造虚假的印象和所谓的现实 —— 这是哲学的分支，涉及知识的本质。**对优化人类知识为已任的哲学们应该对涉及这些产生的这种大规模监视和欺骗操纵，这不仅仅是下一部“新的黑客帝国 Matrix”电影的素材，而是真正的认知战争。**

纽约时报说，为了对私人情报机构在我们社会中扮演的操纵角色有所了解，有必要研究过去几年中一些最重要的秘密数据所揭示的信息。这些重要见解来自 2010 年被一个名叫 LulzSec 的团体（当时该团体被称为“互联网联邦调查局”），其目标是私人情报公司 HBGary Federal。

该组织收到了 75,000 封被曝光的电子邮件，其内容涉及担心 Wikileaks 的曝光行动，美国银行向司法部求助，美国司法部反过来将美国银行转介给游说公司 Hunton 和 Williams，后者又将该银行与一组信息安全公司联合起来，这些公司统称为 Themis 团队。

Themis 团队被有效地引入（包括 HBGary 以及私人情报和安全公司 Palantir Technologies、Berico Technologies 和 Endgame Systems 的团队）**目的是寻找破坏 Wikileaks 和断绝登最信任的著名记者 Glenn Greenwald 的声誉，也就是我们在前言中所描述的：为了继续掩盖真相，当局启动了抹黑模式，试图令揭秘者失信，从而操纵大众的认知。**

你完全可以想像，如果中国当局遇到敢于揭发政治黑幕的人，他们也会这么做，抹黑和构陷几乎是大多数情况下的捷径。

最近几天内的一个热门消息就是，厄瓜多尔总统 Lenin Moreno 前往英国“谈判”，准备将 Julian Assange 交给英国政府。如果实现，将极有可能导致 Wikileaks 主编被引渡到美国，面临死刑或无限期关押终不得审判。从奥巴马政府开始，已经有很多揭秘者遭受了同样的命运，特朗普政府的做法只会更甚。

这一突发消息此前很多人没有想到，因为厄瓜多尔宪法是禁止引渡本国公民的，而 Julian 已经获得了厄瓜多尔公民身份，理论上 Moreno 不能这么做。但是现实是，Moreno 太顺从美国的订单以致于放弃了（准确说是他的政权稳固性）他已经不惜违宪。

延伸阅读：Imminent threat to Julian Assange underscores need for global defence movement

其实有些人已经预先意识到了这一案子的事态正在恶化，因为它是有迹象的，那就是在此消息出现之前的10天左右，网络上忽然出现了很多抹黑的舆论，甚至还有体制内媒体的参与，针对揭秘记者、普利策新闻奖获得者 Glenn Greenwald —— 他是美国最著名的记者之一，因协助斯诺登的披露，长期遭受各种恶意围攻，已移民巴西。

这是一种“要动手了”的暗示，相比下中国网民或许更了解这种模式。

但至少在 2013 年，美国网友对这种操作模式尚未熟知，在纽约时报揭露这件事之前。

延伸阅读：美国的“五毛水军什么样”

纽约时报说，Themis 团队还制定了一项建议，以破坏最著名的批评家之一的可信度，该组织名为 Chamber Watch。这项提案要求首先制作一份“虚假文件，大致类似定期的财务信息”，将其交给这个反对商会的进步团体，然后将该文件作为假文件公开，也就是致钱钱脸，再乘自“辟谣”，以“证明 Chamber Watch 不可信”。

此外，Themis 在这个舆论操纵团队还**建议创建一个“虚假内幕人物”来渗透到反对派组织 Chamber Watch 中**。曝光的电子邮件显示，他们将“创造两个虚假的内幕人物角色，用一个作为杠杆来谴责另一个，同时确认第二个人的合法性。”

曝光电子邮件的证据表明，Themis 团队正在开发一个**“人格管理”系统 —— 一个根据美国空军的特定要求开发的程序，允许一个用户控制多个在线身份（就是人肉水军）以进行舆论引导，在社交媒体空间伪装装易装支持，**纽约时报说，该计划的合同最终授予另一家私人情报公司。

有人以为这是“源代码”电影中的情节吗？不，它是真实的，就存在于现实社会中。纽约时报说，**这是在某种程度上类似于“Psyops”（心理操纵）的使用，学过美国历史的学生们都知道这种东西，几十年来它就是“国家军事战略”的一部分。**

在军方的“非常规战争训练手册”中，Psyops 被定义为“向外国观众传达选定信息和指示的计划行动，以影响他们的情感、动机、客观推理，最终影响外国政府、组织、团体和个人的行为。”

换句话说就是，用欺骗和虚假的现实感来操纵人民，有时比用武力或常规武器强加于其意志，更有效。当然，您可能以选择其视为对敌人的控制“动机、推理和行为”的策略，但别忘了，这也很可能被用于施加在自己人身上。如今你能看到太多的后者正频繁出现。

最重要的是，Psyops（心理操纵）根本不需要由国家政府来实施，完全可以由具有执行这种操纵行为之能力和激励的任何人来执行，对于私人情报承包商，能力是充分的，并且有耀眼的激励 —— 价值数十亿美元的合同。

换句话说就是，你不知道这些承包商的幕后是谁，根本无法“提防”。

当年，在 HBGary 遭遇黑客入侵几个月后，一位名叫 Jeremy Hammond 的芝加哥地区活动家和黑客技术人士，成功入侵了另一家私人情报公司 —— Strategic Forcasting Inc.或叫 Stratfor，并发布了大约 500 万封电子邮件。

这些电子邮件的揭露提供了一个非凡的洞察视角，关于私人情报公司如何看待自己与 C.I.A. 等政府安全机构之间的关系。

然而，这位透明度革命的英雄却被判处十年徒刑！此时严重打击了知情权运动，Jeremy Hammond 的支持者走上街头为其声援。

Hammond's supporters were vocal and numerous. More than 250 people wrote letters to the court to support him.

通过 Hammond 曝光的电子邮件，人们了解到很多内幕，比如在 2004 年向 Stratfor 员工发送的一封电子邮件中，该公司的创始人兼董事长 George Friedman 完全不顾于中央情报局对于他们自己的财务信息，他说：“兰利的每个人都知道我们做过什么……我们现在可以向他们展示，但许他们可以学到点儿东西。”

纽约时报还说，Stratfor 的电子邮件让我们对私人保安公司的世界有了更为清晰的观点，这一认识令人恐惧。

尤其是，泄露的电子邮件显示了监视社会活动人士的事实，监视针对占领运动的抗议者以及与环境组织 Deep Green Resistance 的关系。Stratfor 还参与了其他监测活动，被文章标注为目标的活动家还有印度博帕尔的化学工厂灾难受害者寻求赔偿，其中包括一个名为 Bhopal Medical Appeal 的团体。

更令人惊讶的是，被监测目标还包括 The Yes Men，这是一个讽刺戏仿化学公司的团队，当然与中国的嘴炮不同，该团队在行动后会公开自我辩护，他们曾经制造了一个假的新闻发布会宣布为……

总之，私人情报行业有效地导入 Psyops（心理操纵）以愚弄美国公众，“参与行动计划、将选定的信息传达给外国受众，以影响公众的情感、动机、客观推理，最终、影响人们的行为”。或者正如作者所说，他们正在进行认知战争。

延伸阅读：美国国家通信情报（GCHQ）在2012 年的SigDev 大会上发布的一份幻灯片描述了针对异议目标群体的两种存在形式：“信息作战”和“技术破坏”，其目的被称之为4D：Deny 否定 Disrupt 破坏 Degrade 贬低 Deceive 欺骗……

> 一个希腊词：aletheia，通常被翻译为 the truth，但更恰当地翻译是“披露”或“揭露”——宇宙意思是“不被隐藏的状态”。揭露真相需要……我们进行这种揭露——打败谎言的真相的世界，在第一项任务就是……Wikileaks 和所有……的媒体的本职工作。

这些揭露者正在保护我们免受认知攻击，……我们眼睛上蒙着的黑布……

我们之所以在这里用中文长篇大论……批判性思考在当下的价值……

我们下面的文章中将更多解释为什么……

批判性思考和揭露，我们能做的唯一的事，也是最有效的事。

PS: 原文发表于我们的博客：https://iyouport.wixsite.com/iyouport/blog/…
我们的另一个博客在这里：https://steemit.com/@iyouport
在 Google 关注 iYouPort: https://plus.google.com/b/104314277918209223775/104314277918209223775
在 twitter 关注 iYouPort: https://twitter.com/iyouport_news

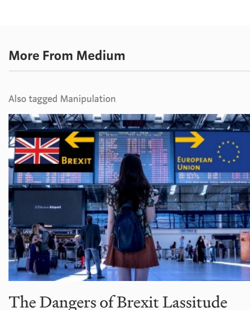
Spy · Political · Manipulation

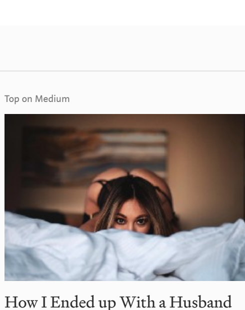
1.6K claps

WRITTEN BY
iYouPort
#AntiCensorship #AntiSurveillance #PressFreedom #Crypto #OSINT #Technology 我方网站：https://www.iyouport.org/

See responses (1)

More From Medium

Also tagged Manipulation

The Dangers of Brexit Lassitude
Simon Newman · Nov 6 · 4 min read

Top on Medium

How I Ended up With a Husband and a Boyfriend.
M. C. Frances · Nov 11 · 11 min read

Top on Medium

Do You Make This Mistake In Conversations?
John P. Weiss in Personal Growth · Oct 24 · 11 min read

Discover Medium
Welcome to a place where words matter. On Medium, smart voices and original ideas take center stage — with no ads in sight. Watch

Make Medium yours
Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. Explore

Become a member
Get unlimited access to the best stories on Medium — and support writers while you're at it. Just $5/month. Upgrade

Medium About Help Legal